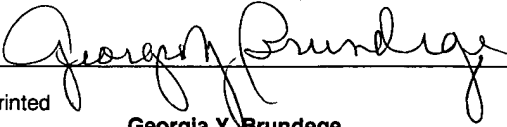





Doc Code: AP.PRE.REQ

PTO/SB/33 (07/05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number (Optional) RSW920010214US1	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR on <u>04/13/2006</u> Signature <u></u> Typed or printed name <u>Georgia Y. Brundage</u>		Application Number 10/015,377	Filed 12/12/2001
		First Named Inventor Ashley Anderson Brock et al.	
		Art Unit 2131	Examiner Longbit Chai
Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.			
This request is being filed with a notice of appeal.			
The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.			
I am the			
<input type="checkbox"/> applicant/inventor.		Signature	
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)		Arthur J. Samodovitz	
<input checked="" type="checkbox"/> attorney or agent of record. Registration number <u>31,297</u>		607-429-4368	
		Telephone number	
<input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____		04/13/2006	
		Date	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.			

<input checked="" type="checkbox"/> *Total of 1 forms are submitted.
--

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 2131
Ashley Anderson Brock et al.	:	Examiner: Longbit Chai
Serial No.: 10/015,377	:	IBM Corporation
Filed: 12/12/2001	:	Intellectual Property Law
Title: INTRUSION DETECTION METHOD	:	Department IQ0A/040-3
AND SIGNATURE TABLE	:	1701 North Street
	:	Endicott, NY 13760

Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

REASONS FOR REQUESTING A PRE-APPEAL BRIEF REVIEW

Claims 21-26 and 31-32 were elected, and rejected under 35 USC 102(a) based on Vaidya (US Patent 6,279,113). Claims 31 and 32 were also found objectionable under 35 USC 112, second paragraph. Appellants respectfully traverse this rejection and objection as follows.

35 USC 102 Rejection

Claim 21 recites a method of detecting intrusions. A plurality of intrusion signatures are stored. A multiplicity of system events having respective signatures are automatically detected. Each of the multiplicity of system event signatures is compared to the plurality of intrusion signatures. A number of times that each of the intrusion signatures matched the system event signatures is recorded. The stored plurality of intrusion signatures are automatically ordered based on how many times each of the intrusion signatures matched the system event signatures, such that the intrusion signature matching the most system event signatures is first in the order. A signature of a subsequent system event is subsequently compared with the plurality of intrusion signatures in the order.

Thus, claim 21 recites automatic ordering of the stored plurality of intrusion signatures based on how many times each of the intrusion signatures matched the system event signatures, such that the intrusion signature matching the most system event signatures is first in the order; and subsequently comparing a signature of a subsequent system event with the plurality of intrusion signatures in the order. The order of the signatures in the list typically impacts the time required to match a system event signature to a signature on the list. Because of the ordering recited in claim 21 (based on past experience), there is a greater likelihood that a subsequent system event signature will match a signature earlier on the list than later. Statistically, this will reduce search time through the order to find a match. This is not taught or suggested by the Prior Art. Vaidya discloses that an attack signature profile might include *expressions* A, B and C. Vaidya also discloses an expression list, for example, including expressions A, B and C. However, the ordering of Vaidya's list is not changed based on how many times there is a match to each expression, and there is no suggestion of this. The Examiner's reliance on Vaidya as teaching this feature of claim 21 represents clear factual error. Also, the Examiner failed to make a prima facie case under 35 USC 102 or 103. Therefore, the rejection of claim 21 under 35 USC 102 should be reversed, and there is no basis to reject claim 21 under 35 USC 103. Appellants also request the PreAppeal Board to render an opinion as to 35 USC 103.

Claims 22 and 23 depend on claim 21. Independent claim 24 distinguishes over Vaidya for the same reasons that claim 21 distinguishes thereover, and claims 25 and 26 depend on claim 24.

Independent claim 31 distinguishes over Vaidya for the same reason that claim 21 distinguishes over Vaidya. In addition, claim 31 recites that one of the system event signatures does not match any of the intrusion signatures and does not correspond to an intrusion, and other of the system event signatures match respective ones of the intrusion signatures. The one system event signature is stored in association with the plurality of intrusion signatures. A number of times that each of the intrusion signatures matches a respective one of the system event signatures is recorded. A number of times that the one system event has occurred is recorded. The stored plurality of intrusion signatures and the one system event signature are subsequently ordered based on the respective number of times that have been recorded for the plurality of intrusion signatures and the one system event signature, such that the signature for which the most number of times has been recorded is first in the order.

Thus, independent claim 31 recites a technique to add a new system event signature, not corresponding to an intrusion, to the list of intrusion signatures. The intrusion signatures and the one new system event signature are ordered based on the number of times they are matched. If the one system event occurs relatively frequently, its signature will be near to the beginning of the order. Statistically, this will reduce search time through the list because the search can terminate when the one system event signature is encountered without searching the remainder of the list. The Examiner did not cite any prior art for this feature of claim 31, so this represents clear error by the Examiner. Also, the Examiner failed to make a prima facie case under 35 USC 102 or 103. Therefore, the rejection of claim 31 under 35 USC 102 should be reversed, and there is no basis to reject claim 31 under 35 USC 103. Appellants also request the PreAppeal Board to render an opinion as to 35 USC 103.

Independent claim 32 distinguishes over Vaidya for the same reason that claim 31 distinguishes over Vaidya.

35 USC 112, Second Paragraph Rejection


The Examiner objected to claims 31 and 32 because of the recitation “storing said one system event signature in association with said plurality of intrusion signatures” in line 8 of claim 31 and line 8 of claim 32. The Examiner asserted that there was no antecedent basis for “said one system event signature”. Appellants respectfully traverse this rejection based on the following.

The antecedent basis for “said one system event signature” is “one of said system event signatures” in line 5 of claim 31 and line 5 of claim 32. (“Said one system event signature” does not refer to “other of said system event signatures” as asserted by the Examiner, because “other” is not the same as “one”.) This represents clear error by the Examiner.

Based on the foregoing, Appellants request that the Pre-Appeal Board reverse all the rejections of the Examiner.

Respectfully submitted,

Dated: April 17, 2006
Telephone: 607-429-4368
Fax: 607-429-4119


Arthur J. Samodovitz
Reg. No: 31,297